Hans Opolka

Central Simple Algebras and Galois Representations of Class Two

Braunschweig : Institut für Analysis und Algebra, 2009

Veröffentlicht: 11.09.2009

http://www.digibib.tu-bs.de/?docid=00029566

CENTRAL SIMPLE ALGEBRAS AND GALOIS REPRESENTATIONS OF CLASS TWO

Hans Opolka
TU Braunschweig
Institut für Analysis und Algebra
Pockelsstraße 14
D - 38106 Braunschweig
e-mail: h.opolka@tu-bs.de

Abstract We investigate class two representations of the absolute Galois group $\mathcal{G}_k$ of a number field k by using central simple algebras which are constructed from symplectic pairings on $\mathcal{G}_k$.

AMS classification 2000: 11R32, 11R34, 11R37, 11R54

Keywords and phrases: Galois theory of number fields, Galois cohomology, algebras

Introduction and statement of results

The basic idea of the present paper is to view a class two representation of the absolute Galois group of a field as a solution of a certain central embedding problem for this Galois group. According to [2] and [7] this embedding problem can be investigated by applying the theory of central simple algebras. Similar methods have been used by the author in previous papers already, see e.g. [12] , [13] , but in situations which are different from the present one or under special assumptions only.

Let us state some of the main results in a preliminary form; for precise definitions and formulations see §2 and §3. For any field k denote by $\mathcal{G}_k$ the absolute Galois group of k, i.e. $\mathcal{G}_k$ is the Galois group $G(\overline{k}/k)$ of a fixed separable algebraic closure $\overline{k}$ of k. Furthermore let W denote the group of all roots of unity in $\mathbb{C}$ and for any positive integer d denote by W_d the group of all roots of unity of order dividing d in $\mathbb{C}$. By a representation of $\mathcal{G}_k$ over $\mathbb{C}$ of degree n we mean a continuous homomorphism $D : \mathcal{G}_k \to GL(n, \mathbb{C})$, where $\mathcal{G}_k$ is regarded as a topological group with respect to the profinite topology and $GL(n, \mathbb{C})$ is regarded as a topological group with respect to the discrete topology. The character of a representation D of $\mathcal{G}_k$ over $\mathbb{C}$, i.e. the function $\mathcal{G}_k \to \mathbb{C}$, $\sigma \mapsto trace(D(\sigma))$, is said to be *rational* over a subfield E of $\mathbb{C}$ if all its values belong to E. Assume that k is a number field. For every place v of k let $\overline{v}$ be an extension of v to $\overline{k}$. Denote by $\mathcal{G}_{k,\overline{v}}$ the decomposition group of $\overline{v}$ and by $I_{k,\overline{v}}$ its inertia group. We often view $\overline{k}$ as being embedded into the union $\mathcal{K}(k, \overline{v})$ of the completions $K_{\overline{v}}$ of all finite subextensions K/k of $\overline{k}/k$. $\mathcal{K}(k, \overline{v})$ is an algebraic closure $\overline{k_v}$ of k_v, and the decomposition group $\mathcal{G}_{k,\overline{v}}$ is isomorphic to the Galois group $G(\overline{k_v}/k_v)$. A representation of $\mathcal{G}_k$ is said to be unramified at a place v of k if for some extension $\overline{v}$ of v to $\overline{k}$ the inertia group $I_{k,\overline{v}}$ is contained in the kernel of D. A representation D of $\mathcal{G}_k$ over $\mathbb{C}$ is said to be of class two if D is irreducible and if the factor group of $\mathcal{G}_k$ modulo the kernel of D is a finite

nonabelian nilpotent group of class two. The following finiteness result will be shown.

Theorem 1 *Let k be a number field. Assume that h is a positive integer and that S is a finite set of places of k which contains all places above h and infinity. Then there are only finitely many isomorphism classes of representations of class two of $\mathcal{G}_k$ which are unramified at all places v of k such that $v \notin S$ and whose characters are rational over the cyclotomic field $\mathbb{Q}(W_h)$.*

Note that in this result the degree of the representations is not prescribed.

In order to state the next result assume that D is a representation of $\mathcal{G}_k$ of class two. Then for all $\sigma, \tau \in \mathcal{G}_k$ the commutator $[D(\sigma), D(\tau)]$ is a scalar matrix $\omega(\sigma, \tau)Id$. In this way we get a continuous symplectic pairing $\omega = \omega_D : \mathcal{G}_k \times \mathcal{G}_k \to \mathbb{C}^*, (\sigma, \tau) \mapsto \omega(\sigma, \tau)$,which is uniquely determined by the set of representations of the form $\lambda \otimes D'$, where D' is any representation isomorphic to D and $\lambda : \mathcal{G}_k \to \mathbb{C}^*$ is any continuous linear character of $\mathcal{G}_k$. The radical of ω is an open subgroup of $\mathcal{G}_k$ which by Galois theory corresponds to a finite Galois subextension K^ω/k of $\overline{k}/k$. Denote by $m(\omega)$ the order of ω. Now assume that k is a number field. For any place v of k denote, as before, by $\overline{v}$ some extension of v to $\overline{k}$. If K/k is a subextension of $\overline{k}/k$ then we denote by $\overline{v}$ also the restriction of $\overline{v}$ to K, and if K/k is Galois with Galois group $G(K/k)$ then $G(K/k)_{\overline{v}}$ denotes the decomposition subgroup of $G(K/k)$ which corresponds to the restriction of $\overline{v}$ to K. For every place v of k denote by $m(\omega_{\overline{v}})$ the order of the restriction $\omega_{\overline{v}}$ of ω to the decomposition group $\mathcal{G}_{k,\overline{v}}$; if $\widetilde{v}$ is another extension of v to $\overline{k}$ then $m(\omega_{\overline{v}}) = m(\omega_{\widetilde{v}})$. For any positive integer d let μ_d denote the group of all roots of unity of order dividing d in $\overline{k}$ and for any multiple $n(\omega)$ of $m(\omega)$ let $S(n(\omega))$ denote the finite set of places of k which consists of all places of k which are ramified in the extension K^ω/k and all places of k which divide $n(\omega)$ and all the infinite places of k. Put $\underline{m}(\omega) := 2 \cdot m(\omega)$ if $m(\omega)$ is even and $\underline{m}(\omega) := m(\omega)$ if $m(\omega)$ is odd.

Definition Let $b(\omega)$ denote the smallest multiple b of $\underline{m}(\omega)$ such that all the congruences $(k(\mu_b)_{\overline{v}} : k(\mu_{\underline{m}(\omega)})_{\overline{v}}) \equiv 0 \bmod(m(\omega_{\overline{v}}))$, $v \in S(m(\omega))$, are satisfied.

The existence of $b(\omega)$ is easy to verify; it follows also from a stronger result in [23] , proof of lemma, p. 192. We will mention examples of nontrivial ω such that $\omega_{\overline{v}}$ is trivial for all places v of k and therefore $b(\omega) = \underline{m}(\omega)$. These examples are related to the Hasse norm principle.

It will be seen later that for every class two representation D of $\mathcal{G}_k$ every subfield E of $\mathbb{C}$ such that the character of D is rational over E contains the cyclotomic field $\mathbb{Q}(W_{m(\omega_D)})$, and we will prove

Theorem 2 *Let k be a number field. Then for every class two representation D of $\mathcal{G}_k$ with symplectic pairing $\omega = \omega_D$ there is a linear character $\lambda : \mathcal{G}_k \to \mathbb{C}^*$ such that the character of the representation $\lambda \otimes D$ is rational over $\mathbb{Q}(W_{2 \cdot b(\omega)})$.*

In §3 we will point out a condition which implies that the linear character $\lambda : \mathcal{G}_k \to \mathbb{C}^*$ in Theorem 2 can be chosen in such a way that the character of $\lambda \otimes D$ is not only rational over $\mathbb{Q}(W_{2\cdot b(\omega)})$ but that $\lambda \otimes D$ is also unramified outside $S(b(\omega))$. This condition is known to hold for $k = \mathbb{Q}$ and in many other situations. We will also discuss an example in the case $k = \mathbb{Q}$ which is related to the Schur index problem for the irreducible characters of a certain finite group and an example in the case $k = \mathbb{Q}(\sqrt[2]{-1})$ which is related to the theory of complex multiplication.

§1. Symplectic pairings, central embedding problems and central simple algebras

For any profinite group $\mathcal{G}$ put $\mathcal{A} := \mathcal{G}/\mathcal{G}'$ where $\mathcal{G}'$ is the closed commutator subgroup of $\mathcal{G}$. Assume that $\omega : \mathcal{A} \times \mathcal{A} \to \mathbb{C}^*$ is a continuous symplectic pairing, i.e. ω is bimultiplicative, symplectic and continuous with respect to the profinite topology on $\mathcal{A}$ and the discrete topology on $\mathbb{C}^*$. It follows that the radical $\mathcal{R}(\omega) := \{\sigma \in \mathcal{A} : \omega(\sigma, \tau) = 1 \text{ for all } \tau \in \mathcal{A}\}$ is a closed normal subgroup of finite index in $\mathcal{A}$. Put $G(\omega) := \mathcal{A}/\mathcal{R}(\omega)$. Then ω induces a nondegenerate symplectic pairing $\varpi : G(\omega) \times G(\omega) \to \mathbb{C}^*$. Denote by $m(\omega)$ the order of ω. The "symplectic pair" $(G(\omega), \varpi)$ can be decomposed as an orthogonal sum of hyperbplic symplectic pairs, and therefore there are maximal $\overline{\omega}$-isotropic subgroups A, B of $G(\omega)$ such that $A \cong B$ and $G(\omega) = A \times B$; see e.g. [25], proof of proposition 6.2. Because of an analogy with physics such a pair of subgroups A, B of $G(\omega)$ is called a *Lagrangian pair* for $(G(\omega), \varpi)$. The continuous symplectic pairings $\omega : \mathcal{A} \times \mathcal{A} \to \mathbb{C}^*$ form a group $PS(\mathcal{A}, \mathbb{C}^*)$ under pointwise defined multiplication. For any profinite group $\mathcal{F}$ and any discrete abelian group M denote by $H^2(\mathcal{F}, M)$ the second cohomology group of $\mathcal{F}$ with respect to the trivial action of $\mathcal{F}$ on M. It is well known that the class $(t) \in H^2(\mathcal{A}, \mathbb{C}^*)$ of an arbitrary central 2-cocycle $t : \mathcal{A} \times \mathcal{A} \to \mathbb{C}^*$ yields the continuous symplectic pairing $\omega_{(t)} : \mathcal{A} \times \mathcal{A} \to \mathbb{C}^*$, where $\omega_{(t)}(\sigma, \tau) := t(\sigma, \tau)/t(\tau, \sigma)$ for all $\sigma, \tau \in \mathcal{A}$, and that the resulting mapping

$$\beta : H^2(\mathcal{A}, \mathbb{C}^*) \to PS(\mathcal{A}, \mathbb{C}^*), \quad (t) \mapsto \omega_{(t)},$$

is an isomorphism. In the case of finite groups this result is shown e.g. in [25] , corollary 2, p.161; it is easily extended to the profinite situation. We note also that for every profinite quotient group $\mathcal{B}$ of $\mathcal{A}$ the inflation homomorphism

$$\inf : H^2(\mathcal{B}, \mathbb{C}^*) \to H^2(\mathcal{A}, \mathbb{C}^*)$$

is injective because every continuous homomorphism of a closed subgroup of $\mathcal{A}$ can be extended to a continuous homomorphism of $\mathcal{A}$ and therefore the corresponding transgression homomorphism in the exact Hochschild-Serre sequence is trivial, which implies the assertion. For every $\omega \in PS(\mathcal{A}, \mathbb{C}^*)$ the preimage

$\beta^{-1}(\omega) \in H^2(\mathcal{A}, \mathbb{C}^*)$ of ω under β is contained in the image of the inflation homomorphism $\inf : H^2(G(\omega), \mathbb{C}^*) \to H^2(\mathcal{A}, \mathbb{C}^*)$; and there is a *central 2-cocycle ε of order $m(\omega)$ for ω*, which by definition means that there is a central 2-cocycle $\varepsilon : G(\omega) \times G(\omega) \to W_{m(\omega)}$ such that the image of $(\varepsilon) \in H^2(G(\omega), W_{m(\omega)})$ under the homomorphism

$$H^2(G(\omega), W_{m(\omega)}) \overset{W_{m(\omega)} \hookrightarrow \mathbb{C}^*}{\to} H^2(G(\omega), \mathbb{C}^*) \overset{\inf}{\hookrightarrow} H^2(\mathcal{A}, \mathbb{C}^*)$$

is $\beta^{-1}(\omega)$. In fact, choose a Lagrangian pair (A, B) for $(G(\omega), \varpi)$. Then the mapping $\varepsilon : G(\omega) \times G(\omega) \to W_{m(\omega)}$ defined by $\varepsilon(ab, a'b') := \omega(a, b')$ for all $a, a' \in A$, $b, b' \in B$, is bimultiplicative and satisfies $\varepsilon(\sigma, \tau)/\varepsilon(\tau, \sigma) = \omega(\sigma, \tau)$ for all $\sigma, \tau \in G(\omega)$, hence is a central 2-cocycle of order $m(\omega)$ for ω. For every central 2-cocycle ε of order $m(\omega)$ for ω and any multiple $\widetilde{m}$ of $m(\omega)$ denote by

$$1 \to W_{\widetilde{m}} \to E(\varepsilon_{m(\omega),\widetilde{m}}) \to G(\omega) \to 1$$

the group extension which is defined by the cocycle

$$\varepsilon_{m(\omega),\widetilde{m}} : G(\omega) \times G(\omega) \overset{\varepsilon}{\to} W_{m(\omega)} \hookrightarrow W_{\widetilde{m}} \ .$$

Using [7], section 1, we get

(1.1) **Proposition** *The embedding problem $\mathfrak{E}(\omega, \varepsilon_{m(\omega),\widetilde{m}})$ for $\mathcal{G}$ which is defined by this group extension is solvable, i.e. there is a homomorphism $\phi : \mathcal{G} \to E(\varepsilon_{m(\omega),\widetilde{m}})$ such that ϕ composed with the epimorphism $E(\varepsilon_{m(\omega),\widetilde{m}}) \to G(\omega)$ yields the natural epimorphism $\mathcal{G} \to G(\omega) = \mathcal{G}/\mathcal{R}(\omega)$, if and only if $\left(\varepsilon_{m(\omega),\widetilde{m}}\right)$ is contained in the kernel of the inflation homomorphism* $\inf : H^2(G(\omega), W_{\widetilde{m}}) \to H^2(\mathcal{G}, W_{\widetilde{m}})$.

Some profinite groups $\mathcal{G}$ are known which have the so called inflation property:

(1.2) **Inflation property** *The inflation homomorphism* $\inf : H^2(\mathcal{A}, W) \to H^2(\mathcal{G}, W)$ *is trivial.*

We note that $H^2(\mathcal{G}, W) \cong H^2(\mathcal{G}, \mathbb{C}^*)$ and get the following well known result which is important for the purposes of the present paper.

(1.3) **Proposition** *The inflation property (1.2) implies that for any $\omega \in PS(\mathcal{A}, \mathbb{C}^*)$ there is a central 2-cocycle ε of order $m(\omega)$ for ω and a multiple $\widetilde{m}$ of $m(\omega)$ such that the embedding problem $\mathfrak{E}(\omega, \varepsilon_{m(\omega),\widetilde{m}})$ for $\mathcal{G}$ is solvable.*

For the sake of completeness we recall the easy proof : Let $\epsilon : G(\omega) \times G(\omega) \to W_{m(\omega)}$ be a central 2-cocycle of order $m(\omega)$ for ω. The inflation property (1.2) implies that there is a continuous function $\alpha : \mathcal{G} \to W$ such that

$\varepsilon(\sigma\mathcal{R}(\omega),\tau\mathcal{R}(\omega)) = \alpha(\sigma)\alpha(\tau)/\alpha(\sigma\tau)$ for all $\sigma,\tau \in \mathcal{G}$. Hence $\alpha^{m(\omega)} : \mathcal{G} \to W$ is a continuous homomorphism, of order l say. Then for $\widetilde{m} := m(\omega)\cdot l$ the image of $\left(\varepsilon_{m(\omega),\widetilde{m}}\right) \in H^2(G(\omega), W_{\widetilde{m}})$ under the inflation homomorphism inf : $H^2(G(\omega), W_{\widetilde{m}}) \to H^2(\mathcal{G}, W_{\widetilde{m}})$ is trivial. The assertion follows by applying (1.1).

Let k be a field of characteristic 0 with algebraic closure $\overline{k}$ and absolute Galois group $\mathcal{G} = \mathcal{G}_k := G(\overline{k}/k)$. Then $\mathcal{A} := \mathcal{A}_k := \mathcal{G}_k/\mathcal{G}_k^{'}$ is the Galois group of the maximal abelian subextension k^{ab}/k of $\overline{k}/k$. For any $\omega \in PS(\mathcal{A}_k, \mathbb{C}^*)$ denote by $K^\omega \subset k^{ab}$ the fix field corresponding to $\mathcal{R}(\omega)$ by Galois theory; so $G(\omega) = G(K^\omega/k)$ is the Galois group of K^ω/k. We identify the group $\overline{\mu} = \mu(\overline{k})$ of all roots of unity in $\overline{k}$ with the group W of all roots of unity in $\mathbb{C}^*$ and thereby we get, for every positive integer d, an isomorphism of the group $\mu_d = \mu_d(\overline{k})$ of roots of unity of order dividing d in $\overline{k}^*$ onto W_d. Let $\varepsilon : G(\omega)\times G(\omega) \to W_{m(\omega)} \cong \mu_{m(\omega)}$ be a central 2-cocycle of order $m(\omega)$ for ω. Put $G_{m(\omega)} := G(K^\omega(\mu_{m(\omega)})/k(\mu_{m(\omega)}))$ and denote by $\varepsilon_{/m(\omega)}$ the restiction of ε to $G_{m(\omega)} \times G_{m(\omega)}$. Then the crossed product algebra

$$A(\omega,\varepsilon) := (K^\omega(\mu_{m(\omega)})/k(\mu_{m(\omega)}, \varepsilon_{/m(\omega)}),$$

which is defined by $\varepsilon_{/m(\omega)}$, is a central simple $k(\mu_{m(\omega)})$-algebra of exponent dividing $m(\omega)$; see e.g. [5] ,V, §1. We will make use of the following well known result of Tate [22]; for a proof see e.g. [16] , §6.

Theorem (Tate) *If k is a local or global number field then the cohomology group $H^2(\mathcal{G}_k, W)$ is trivial.*

From this result it is obvious that the inflation property (1.2) holds for $\mathcal{G} = \mathcal{G}_k$ where k is a local or global number field. We recall that for a number field k every solvable embedding problem with abelian kernel for $\mathcal{G}_k$ has a proper, i.e. surjective, solution; comp. [8] or [7] , (6.7), p. 101, and therefore in the number field case we assume that solutions of our central embedding problems are always proper.

(1.4) **Proposition** *Assume that k is a number field and let $\omega \in PS(\mathcal{A}_k, \mathbb{C}^*)$. Denote by $b(\omega)$ the integer defined in the introduction. Assume that ε is a bimultiplicative cocycle of order $m(\omega)$ for ω. Then $k(\mu_{b(\omega)})$ is a splitting field for $A(\omega,\varepsilon)$.*

Proof: For every place v of k and any extension $\overline{v}$ of v to $\overline{k}$ denote by $A_{\overline{v}} = A(\omega,\varepsilon)_{\overline{v}}$ the central simple $k(\mu_{m(\omega)})_{\overline{v}}$-algebra $k(\mu_{m(\omega)})_{\overline{v}} \otimes A(\omega,\varepsilon)$. At first we show that the exponent of $k(\mu_{\underline{m}(\omega)})_{\overline{v}} \otimes A(\omega,\varepsilon)_{\overline{v}}$ divides the order $m(\omega_{\overline{v}})$ of the restriction of ω to $\mathcal{G}_{k,\overline{v}}$. In order to see this we modify an argument in [13], proof of (1.4). Since $\omega^{m(\omega_{\overline{v}})}$ is trivial on $G(K^\omega/k)_{\overline{v}}$ there is a function $\alpha_{\overline{v}} : G(K^\omega/k)_{\overline{v}} \to W \cong \overline{\mu}$ such that $\varepsilon^{m(\omega_{\overline{v}})}(\sigma,\tau) = \alpha_{\overline{v}}(\sigma)\alpha_{\overline{v}}(\tau)/\alpha_{\overline{v}}(\sigma\tau)$ for all

$\sigma, \tau \in G(K^\omega/k)_{\overline{v}}$. Then, since ε is bimultiplicative and since the exponent of $G(K^\omega/k)$ divides $m(\omega)$, we have

$$\alpha_{\overline{v}}(\sigma)^{\underline{m}(\omega)} = \prod_{i=1}^{\underline{m}(\omega)} \varepsilon^{m(\omega_{\overline{v}})}(\sigma, \sigma^i) = \varepsilon(\sigma,\sigma)^{m(\omega_{\overline{v}})(\underline{m}(\omega)(\underline{m}(\omega)+1)/2)} = 1$$

for all $\sigma \in G(K^\omega/k)_{\overline{v}}$. Therefore $\varepsilon^{m(\omega_{\overline{v}})}$ splits as a Galois cocycle over $k(\mu_{\underline{m}(\omega)})_{\overline{v}}$. According to the "multiplication theorem" for crossed product algebras, see [5], V, §2, Satz 1, this implies that $k(\mu_{\underline{m}(\omega)})_{\overline{v}}$ is a splitting field of the $m(\omega_{\overline{v}})$-fold tensor product of $k(\mu_{\underline{m}(\omega)})_{\overline{v}} \otimes A_{\overline{v}}$, and therefore the exponent of $k(\mu_{\underline{m}(\omega)})_{\overline{v}} \otimes A_{\overline{v}}$ divides $m(\omega_{\overline{v}})$. Hence the local theory of central simple algebras implies that the field $k(\mu_{b(\omega)})_{\overline{v}}$ splits $A_{\overline{v}}$ for all $v \in S(m(\omega))$, comp. [5], VII, §2, Satz 4. And $A_{\overline{v}}$ splits for all $v \notin S(\omega)$ because the extension $K^\omega(\mu_{m(\omega)})/k(\mu_{m(\omega)})$ is unramified at all places which extend the places $v \notin S(m(\omega))$ and because all values of the cocycle ε are roots of unity; comp. [5] , VII, §1. Therefore by the local global principle in the theory of central simple algebras over number fields, comp. [5] ,VII, §5, Satz 1, the field $k(\mu_{b(\omega)})$ splits the central simple $k(\mu_{m(\omega)})$-algebra $A(\omega, \varepsilon)$.

If $\overline{\omega} \in PS(G(\omega), \mathbb{C}^*)$ belongs to the kernel $\mathcal{H}(K^\omega/k)$ of the localization map $PS(G(\omega), \mathbb{C}^*) \to \prod_v PS(G(\omega)_{\overline{v}}, \mathbb{C}^*)$, we have $m(\omega_{\overline{v}}) = 1$ for all places v of k. So (1.4) implies the following result which is implicit in [13], (1.4), and which is related to a result in [21], (3.4.10), p. 101, on central extensions defined by the obstruction to the validity of the Hasse norm principle for abelian extensions.

(1.5) **Proposition** *If* $\overline{\omega} \in \mathcal{H}(K^\omega/k)$ *is nontrivial, then* $b(\omega) = \underline{m}(\omega)$.

In order to explain the relation of this result to the Hasse norm principle we recall that according to [3] , § 20, Theorem 20.6, p. 101, and [23] , p. 198, for every finite Galois extension K/k of number fields the kernel of the localization homomorphism

$$H^2(G(K/k), \mathbb{C}^*) \to \prod_v H^2(G(K/k)_{\overline{v}}, \mathbb{C}^*)$$

is dual to the group

$$\mathcal{K}(K/k) := \frac{\{a \in k^* : a \text{ is a norm locally everywhere in } K/k\}}{\{a \in k^* : a \text{ is a norm in } K/k\}},$$

which is the obstruction to the validity of the Hasse norm principle for K/k. Using for instance example 1 on p. 297 in [15] it is easy to construct examples of symplectic pairings ω such that the assumption in (1.5) is satisfied. Namely assume that K/k is a Galois extension with Galois group $G(K/k)$ isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for a prime number p such that there is no finite place of k which

is the power of a place of K and let ω be a symplectic pairing on $\mathcal{G}_k$ which is inflated from a symplectic pairing $\overline{\omega}$ of order p on $G(K/k)$. Then $K = K^\omega$ and $\overline{\omega} \in \mathcal{H}(K^\omega/k)$.

For other relations between symplectic pairings and the Hasse norm principle see [15], especially §5.

Now we relate the algebra $A(\omega, \varepsilon)$ to the central embedding problem $\mathfrak{E}(\omega, \varepsilon)$ for $\mathcal{G}_k$. For this purpose we recall first that for any positive integer d and any finite set of places S of the number field k the triple (k, d, S) is said to be in the *special case*, if S contains all places v above 2 such that for $d = 2^t m$ with m odd the extension $k_v(\mu_{2^t})/k_v$ is not cyclic; comp. [11], p. 90, and [1], p. 96. Obviously, if d is odd or if k contains a root of unity of order 4, then the triple (k, d, S) is not in the special case.

For every $\omega \in PS(\mathcal{A}_k, \mathbb{C}^*)$ and any multiple $n(\omega)$ of $m(\omega)$ define $\overline{n}(\omega) := 2 \cdot n(\omega)$, if the triple $(k, n(\omega), S(n(\omega)))$ is in the special case, and $\overline{n}(\omega) := n(\omega)$ otherwise; here $S(n(\omega))$ is the finite set of all places of k which are ramified in K^ω/k and all places of k dividing $n(\omega)$ and all infinite places of k.

(1.6) **Proposition** *Assume that k is a number field. Let $\omega \in PS(\mathcal{A}_k, \mathbb{C}^*)$ and let ε be a central 2-cocycle of order $m(\omega)$ for ω. Assume that $n(\omega)$ is a multiple of $m(\omega)$ such that $k(\mu_{n(\omega)})$ is a splitting field for $A(\omega, \varepsilon)$. Then the central embedding problem $\mathfrak{E}(\omega, \varepsilon_{m(\omega),\overline{n}(\omega)})$ for $\mathcal{G}_k$ is solvable.*

Applying (1.4) this result implies

(1.7) **Corollary** *Assume that k is a number field. Let $\omega \in PS(\mathcal{A}, \mathbb{C}^*)$ and let ε be a central 2-cocycle for ω of order $m(\omega)$. Then the central embedding problem $\mathfrak{E}(\omega, \varepsilon_{m(\omega),\overline{b}(\omega)})$ for $\mathcal{G}_k$ is solvable.*

Proof of (1.6): It follows from [7], section 5, that all the central embedding problems for the decomposition groups $\mathcal{G}_{k,\overline{v}}$, v any place of k, which arise from the central embedding problem $\mathfrak{E}(\omega, \varepsilon_{m(\omega),n(\omega)})$ for $\mathcal{G}_k$, are solvable. Therefore according to [7], section 1, the image of $\left(\varepsilon_{m(\omega),n(\omega)}\right) \in H^2(G(\omega), \mu_{n(\omega)})$ under the inflation homomorphism $\inf : H^2(G(\omega), \mu_{n(\omega)}) \to H^2(\mathcal{G}_k, \mu_{n(\omega)})$ is contained in the kernel of the localization homomorphism

$$H^2(\mathcal{G}_k, \mu_{n(\omega)}) \to \prod_v H^2(\mathcal{G}_{k,\overline{v}}, \mu_{n(\omega)}).$$

The global duality theorem of Tate and Poitou [14], [22] implies that this kernel is dual to $\kappa(k, n(\omega))$ where for any positive integer d

$$\kappa(k, d) := \{\alpha \in k^* : \alpha \in k_v^d \text{ for all places } v \text{ of } k\}/(k^*)^d,$$

Denote by S_d a finite set of places of k which contains all places dividing d. $\kappa(k,d)$ is known to be trivial if the triple (k,d,S_d) is not in the special case and of order at most 2 in any case, see [1] , p. 96 ff. It is well known that the restriction of the homomorphism

$$H^2(\mathcal{G}_k,\mu_{n(\omega)}) \overset{\mu_{n(\omega)}\hookrightarrow\mu_{2\cdot n(\omega)}}{\longrightarrow} H^2(\mathcal{G}_k,\mu_{2\cdot n(\omega)})$$

to the kernel of the above localization homomorphism is dual to the homomorphism $\kappa(k,2\cdot n(\omega))\to\kappa(k,n(\omega))$ induced by $(k^*)^{2n(\omega)}\hookrightarrow(k^*)^{n(\omega)}$, which is trivial. The assertion follows.

For any positive integer n and any finite set of places S of k which contains all places above n and infinity define

$$U(n,S):=\left\{\begin{array}{r} a\in k^*:(a)=\mathfrak{a}^{\,n} \text{ for some fractional ideal } \mathfrak{a} \text{ of } k, \\ \text{and } a\in(k_v^*)^n \text{ for all } v\in S \end{array}\right\}.$$

(1.8) **Remark** It follows from [11], (8.2), S.104, that the condition $U(n,S)=(k^*)^n$ holds for $k=\mathbb{Q}$ and arbitrary n; and the remarks in [11] , p. 103, following (8.1), show that the condition $U(n,S)=(k^*)^n$ holds also if n is a power of an odd prime number p such that the class number of the cyclotomic extension $k(\mu_n)$ is prime to p.

[11] , (8.1), p.102/103 implies

(1.9) **Remark** For every $\omega\in PS(\mathcal{A},\mathbb{C}^*)$ and every central 2-cocycle ε of order $m(\omega)$ for ω the condition $U(\overline{b}(\omega),S(\overline{b}(\omega)))=(k^*)^{\overline{b}(\omega)}$ assures that the central embedding problem $\mathfrak{E}(\omega,\varepsilon_{m(\omega),\overline{b}(\omega)})$ for $\mathcal{G}_k$ has a solution which is unramified outside $S(b(\omega))$.

In the following examples symplectic pairings ω and upper bounds for $b(\omega)$ are constructed.

(1.10) **Examples** (a) Assume that $k=\mathbb{Q}$. Let $\omega\in PS(\mathcal{A}_{\mathbb{Q}},\mathbb{C}^*)$. Then by the Kronecker-Weber theorem, see e.g. [1] , Chapter 8, Theorem 6, p. 74, there is a positive integer f such that the abelian extension $K^\omega/\mathbb{Q}$ is contained in the cyclotomic extension $\mathbb{Q}(\mu_f)/\mathbb{Q}$. The smallest f with this property is denoted by $f(\omega)$ and is called the *conductor of* ω. Denote by $g(\omega)$ the lcm of $f(\omega)$ and $m(\omega)$. Then obviously the cyclotomic field $\mathbb{Q}(\mu_{g(\omega)})$ is a splitting field for the central simple $\mathbb{Q}(\mu_{m(\omega)})$-algebra $A(\omega,\varepsilon)=(K^\omega(\mu_{m(\omega)})/\mathbb{Q}(\mu_{m(\omega)}),\varepsilon_{/m(\omega)})$ for every central 2-cocycle ε of order $m(\omega)$ for ω, and therefore according to (1.6), (1.8) and (1.9) the central embedding problem $E(\omega,\varepsilon_{m(\omega),\overline{g}(\omega)})$ for $\mathcal{G}_{\mathbb{Q}}$ has a solution which is unramified outside $S(\overline{g}(\omega))$. This observation is closely related to theorem 3, p. 242, in [6] and theorem 1.4, p. 349, in [17] .

Note that there are some restrictions for a natural number to be the conductor of a symplectic pairing $\omega \in PS(\mathcal{A}_{\mathbb{Q}}, \mathbb{C}^*)$. Namely, since $G(\omega) = G(K^\omega/\mathbb{Q})$ is isomorphic to a direct product of isomorphic abelian groups, the Galois group of the extension $\mathbb{Q}(\mu_{f(\omega)})/\mathbb{Q}$ is not cyclic and its order $\varphi(f(\omega))$ is divisible by a square. Note also that for $k = \mathbb{Q}$ the crossed product algebra $A(\omega, \varepsilon)$ is a so called *cyclotomic algebra* in the sense of [24], Chapter 2, and therefore is isomorphic to a simple component of a group algebra of a finite group H over $\mathbb{Q}(\mu_{m(\omega)})$; in fact, H can be taken to be any group extension

$$1 \to \mu_{g(\omega)} \to H \to G(\mathbb{Q}(\mu_{g(\omega)})/\mathbb{Q}(\mu_{m(\omega)})) \to 1$$

corresponding to the 2-cocycle class

$$\inf((\varepsilon_m)) \in H^2(G(\mathbb{Q}(\mu_{g(\omega)})/\mathbb{Q}(\mu_{m(\omega)})), \mu_{g(\omega)});$$

comp. [24], chapter 2. So one can apply results about splitting fields of representations of finite groups in the present situation. For instance, applying a result of L. Solomon, see e.g. [9], (10.14), p. 168/169, one finds that the field $\mathbb{Q}(\mu_{2l}, \mu_{m(\omega)})$, where l is the product of all prime divisors of $|H| = g(\omega)\varphi(g(\omega))/\varphi(m(\omega))$, splits $A(\omega, \varepsilon)$; here φ denotes the Euler function. It is easy to construct examples where the degree of the last mentioned splitting field $\mathbb{Q}(\mu_{2l}, \mu_{m(\omega)})$ is strictly smaller than the degree of the splitting field $\mathbb{Q}(\mu_{g(\omega)})$ given above. For instance, the Galois group $G(\mathbb{Q}(\mu_{63})/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/9\mathbb{Z})^*$ is a direct product of two cyclic groups of order 6, and therefore carries a nondegenerate symplectic pairing ω of order $m(\omega) = 6$. And $g(\omega) = \mathrm{lcm}(m(\omega), f(\omega)) = \mathrm{lcm}(6, 63) = 2 \cdot 7 \cdot 9$, $\varphi(g(\omega))/\varphi(m(\omega)) = 3 \cdot 6$, $2 \cdot l = 4 \cdot 3 \cdot 7$, hence $(\mathbb{Q}(\mu_{g(\omega)}) : \mathbb{Q}(\mu_{m(\omega)})) = 18$ and $(\mathbb{Q}(\mu_{2l}, \mu_{m(\omega)}) : \mathbb{Q}(\mu_{m(\omega)})) = 12$.

(b) Assume that $k = \mathbb{Q}(\sqrt[3]{-1})$. In this case it is well known from the theory of complex multiplication, see [10], part two, Chapter 10, §1, Theorem 2, that every abelian extension is contained in the field $k(X_f)$ for some positive integer f where X_f denotes the group of torsion points over $\overline{\mathbb{Q}}$ of the elliptic curve $X : y^2 = x^3 + x$; comp. also [19], chapter 8, for an elementary discussion of this result. It follows from the general theory of elliptic curves over number fields that $k(X_f)$ contains μ_f, see [18], III, §8, Corollary 8.1.1. Moreover since 2 is the only prime number which divides the discriminant of X the extension $k(X_f)/k$ is unramified outside the set of places of k which divide 2 and f, see [18], VII, §7, Theorem 7.1. And the Galois group $G(k(X_f)/k)$ is isomorphic to the group of units $(A/fA)^*$ of the quotient ring A/fA, where $A = \mathbb{Z}[\sqrt[3]{-1}]$ is the ring of Gaussian integers, see [10], Chapter 10, §4, Theorem 8. If f is a prime number $\equiv 3 \bmod 4$ then A/fA is a finite field, hence the Galois group $G(k(X_f)/k) \cong (A/fA)^*$ is cyclic and therefore does not carry nontrivial symplectic pairings. However if $f = p$ is a prime $\equiv 1 \bmod 4$ then p splits in A as a product of complex conjugate prime elements; hence $G(k(X_p)/k) \cong (A/fA)^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$ has nontrivial symplectic pairings ω of order $m(\omega)$ dividing $p-1$ such that $K^\omega \subset k(X_p)$. So assume that p is a prime number

$\equiv 1 \bmod 4$. Fix a nontrivial symplectic pairing ω on $G(k(X_p)/k)$ of order $m(\omega)$ dividing $p-1$, and let ε be a central 2-cocycle of order $m(\omega)$ for ω. There is a positive integer r such that the field $k(\mu_{(p-1)^r})$ splits the central simple $k(\mu_{m(\omega)})$-algebra $A(\omega,\varepsilon)$. Therefore according to (1.6) the central embedding problem $\mathfrak{E}(\omega, \varepsilon_{m(\omega),\overline{(p-1)^r}})$ for $\mathcal{G}_k$ is solvable.

§2. **Algebraic description of class two representations**

Let $\mathcal{G}$ be a profinite group. In this section we give a description of class two representations of $\mathcal{G}$ which is based on Clifford's theory [4]. By a linear resp. projective representation of $\mathcal{G}$ we mean a continuous homomorphism $D : \mathcal{G} \to GL(n,\mathbb{C})$ resp. $P : \mathcal{G} \to PGL(n,\mathbb{C})$ for some positive integer n which is called the degree of D resp. P; here $\mathcal{G}$ is regarded as a topological group with respect to the profinite topology and $GL(n,\mathbb{C})$ resp. $PGL(n,\mathbb{C})$ is regarded as a topological group with resprect to the discrete topology. The kernel of any linear or projective representation of $\mathcal{G}$ is a closed normal subgroup of finite index in $\mathcal{G}$. The character of a linear representation D of $\mathcal{G}$, i.e. the function $\mathcal{G} \to \mathbb{C}$, $\sigma \mapsto trace(D(\sigma))$, is said to be *rational* over a subfield E of $\mathbb{C}$ if all its values belong to E. A linear representation $D : \mathcal{G} \to GL(n,\mathbb{C})$ is said to be of class two if D is irreducible and if the image of the corresponding projective representation $\overline{D} : \mathcal{G} \stackrel{D}{\to} GL(n,\mathbb{C}) \to PGL(n,\mathbb{C})$ is a nontrivial abelian group, or, what amounts to the same, if the finite group $\mathcal{G}/Ker(D)$ is a nonabelian nilpotent group of class two. By a linear character of $\mathcal{G}$ we mean a linear representation of $\mathcal{G}$ of degree 1.

Asume now that $\mathcal{G}$ has the inflation property (1.2). Using the profinite version of the Hochschild-Serre exact sequence, see e.g. [20], Chapter II, §4, we see that every $\omega \in PS(\mathcal{A},\mathbb{C}^*)$ is *transgressive*, i.e. there is a $G(\omega)$-invariant linear character $\chi : \mathcal{R}(\omega) \to \mathbb{C}^*$ such that the image of χ under the composition of the transgression homomorphism

$$tr : Hom(\mathcal{R}(\omega),\mathbb{C}^*)^{G(\omega)} \to H^2(G(\omega),\mathbb{C}^*),$$

which is defined by the group extension $1 \to \mathcal{R}(\omega) \to \mathcal{G} \to G(\omega) \to 1$, and the isomorphism $\beta : H^2(G(\omega),\mathbb{C}^*) \to PS(G(\omega),\mathbb{C}^*)$, which was explained in §1, is equal to ω. We call any $G(\omega)$-invariant linear character $\chi : \mathcal{R}(\omega) \to \mathbb{C}^*$ with this property *a central character for* ω and the pair (ω,χ) a *central pair* of $\mathcal{G}$. For such a central pair (ω,χ) Clifford´s theory [4] implies that the induced representation $Ind^{\mathcal{G}}_{\mathcal{R}(\omega)}(\chi)$ is isomorphic to the n-fold direct sum of an irreducible linear representation $D = D(\omega,\chi)$ of $\mathcal{G}$ of degree n, where $n = (\mathcal{G} : \mathcal{R}(\omega))^{1/2}$, and that the restriction of $D(\omega,\chi)$ to $\mathcal{R}(\omega)$ is isomorphic to the n-fold sum of χ :

$$(2.1)\quad Ind^{\mathcal{G}}_{\mathcal{R}(\omega)}(\chi) \cong n\cdot D(\omega,\chi),\ Res^{\mathcal{G}}_{\mathcal{R}(\omega)}(D(\omega,\chi)) \cong n\cdot\chi,\ n = (\mathcal{G} : \mathcal{R}(\omega))^{1/2}$$

It follows that for $m(\omega) \neq 1$ the image of the projective representation defined by $D(\omega, \chi)$ is a nontrivial abelian group and therefore $D(\omega, \chi)$ is of class two. Moreover, the formulas in (2.1) show that the character of $D(\omega, \chi)$ is rational over the cyclotomic field $\mathbb{Q}(W_{m(\chi)})$ where $m(\chi)$ is the order of χ. Since the order $m(\omega)$ of ω divides the order $m(\chi)$ of any central character χ for ω the field $\mathbb{Q}(W_{m(\omega)})$ is contained in $\mathbb{Q}(W_{m(\chi)})$. (2.1) implies also that every subfield E of $\mathbb{C}$ over which the character of $D(\omega, \chi)$ is rational contains all values of χ. Furthermore, two central pairs $(\omega, \chi), (\omega', \chi')$ of $\mathcal{G}$ coincide if and only if $D(\omega, \chi) \cong D(\omega', \chi')$. Conversely, for every class two representation D of $\mathcal{G}$ there is a central pair (ω, χ) of $\mathcal{G}$ such that $D \cong D(\omega, \chi)$. In fact, by Schur's lemma the kernel of the projective representation $\overline{D} : \mathcal{G} \xrightarrow{D} GL(n, \mathbb{C}) \to PGL(n, \mathbb{C})$ arising from D is equal to $\mathcal{R}(\omega)$ where $\omega : \mathcal{A} \times \mathcal{A} \to \mathbb{C}^*$ is the symplectic commutator pairing given by

$$\omega(\sigma \bmod \mathcal{G}', \tau \bmod \mathcal{G}') \cdot Id := [D(\sigma), D(\tau)], \quad \sigma, \tau \in \mathcal{G},$$

and the restriction of D to $\mathcal{R}(\omega)$ is isomorphic to $n \cdot \chi$, where χ is a central character for ω; for the case of finite groups this is implicit in [25], (1.4). Hence by Frobenius reciprocity $n = (\chi, Res^{\mathcal{G}}_{\mathcal{R}(\omega)}(D)) = (Ind^{\mathcal{G}}_{\mathcal{R}(\omega)}(\chi), D)$, and therefore $Ind^{\mathcal{G}}_{\mathcal{R}(\omega)}(\chi) \cong n \cdot D$ which implies $D \cong D(\omega, \chi)$. Altogether we have shown

(2.2) **Proposition** *Assume that $\mathcal{G}$ has the inflation property (1.2). Then the assignment $(\omega, \chi) \mapsto D(\omega, \chi)$ induces a bijective correspondence between the set of central pairs (ω, χ) of $\mathcal{G}$ with nontrivial ω and the set of isomorphism classes of class two representations of $\mathcal{G}$. The character of every representation $D(\omega, \chi)$ is rational over the cyclotomic field $\mathbb{Q}(W_{m(\chi)})$, and every subfield E of $\mathbb{C}$ over which the character of $D(\omega, \chi)$ is rational contains the cyclotomic field $\mathbb{Q}(W_{m(\chi)})$; moreover, $\mathbb{Q}(W_{m(\chi)})$ contains $\mathbb{Q}(W_{m(\omega)})$.*

Two linear representations D_1, D_2 of $\mathcal{G}$ are said to belong to the same *genus* if there is a linear character λ of $\mathcal{G}$ such that $D_2 \cong \lambda \cdot D_1$. This is an equivalence relation which is compatible with the class two property. If $D_1 \cong D(\omega_1, \chi_1)$, $D_2 \cong D(\omega_2, \chi_2)$ and $D_2 \cong \lambda \cdot D_1$ for some linear character λ of $\mathcal{G}$ then $\overline{D_2} \cong \overline{D_1}$, $\omega_2 = \omega_1 = \omega$ and $\chi_2 = Res^{\mathcal{G}}_{\mathcal{R}(\omega)}(\lambda) \cdot \chi_1$. Conversely, if $\omega_2 = \omega_1 = \omega$ and if χ_2, χ_1 are central characters for ω, then the Hochschild-Serre exact sequence shows that there is a linear character λ of $\mathcal{G}$ such that $\chi_2 = Res^{\mathcal{G}}_{\mathcal{R}(\omega)}(\lambda) \cdot \chi_1$, and then by Frobenius reciprocity $Ind^{\mathcal{G}}_{\mathcal{R}(\omega)}(\chi_2) \cong \lambda \cdot Ind^{\mathcal{G}}_{\mathcal{R}(\omega)}(\chi_1)$ which implies $D(\omega_2, \chi_2) \cong \lambda \cdot D(\omega_1, \chi_1)$. These considerations prove

(2.3) **Proposition** *Assume that $\mathcal{G}$ has the inflation property (1.2). Then the assignment $\omega \mapsto$genus of $D(\omega, \chi)$, where χ is any central character for ω,*

gives a bijective correspondence between the nontrivial elements in $PS(\mathcal{A},\mathbb{C}^*)$ *and the set of genera of class two representations of* $\mathcal{G}$.

Finally we connect the central embedding problems which were considered in §1 with central charcters.

(2.4) **Lemma** *Assume that* $\mathcal{G}$ *has the inflation property (1.2). Let* $\omega \in PS(\mathcal{A},\mathbb{C}^*)$ *and let* ε *be a central 2-cocycle for* ω *of order* $m(\omega)$. *Furthermore, let* $n(\omega)$ *be a multiple of* $m(\omega)$ *such that the central embedding problem* $\mathfrak{E}(\omega,\varepsilon_{m(\omega),n(\omega)})$ *for* $\mathcal{G}$ *is solvable. Then there is a central character* χ *of order* $n(\omega)$ *for* ω.

Proof: The argument is based on [7], 2.1, p. 84. The solvability of the embedding problem implies that $\inf(\varepsilon_{m(\omega),n(\omega)}) \in H^2(\mathcal{G},\mu_{n(\omega)})$ is trivial. Applying the Hochschild-Serre exact sequence

$$1 \to Hom(G(\omega),\mu_{n(\omega)}) \overset{\inf}{\to} Hom(\mathcal{G},\mu_{n(\omega)}) \overset{res}{\to} Hom(\mathcal{R}(\omega),\mu_{n(\omega)})^{G(\omega)} \overset{tr}{\to}$$

$$\overset{tr}{\to} H^2(G(\omega),\mu_{n(\omega)}) \overset{\inf}{\to} H^2(\mathcal{G},\mu_{n(\omega)})$$

we see that there is a $G(\omega)$-invariant character $\chi : \mathcal{R}(\omega) \to \mu_{n(\omega)}$ which is mapped onto $(\varepsilon_{m(\omega),n(\omega)}) \in H^2(G(\omega),\mu_{n(\omega)})$ under the transgression homomorphism tr. The assertion follows.

(2.5) **Example** The condition that the character of a class two representation D of $\mathcal{G}$ is rational over $\mathbb{Q}$ implies that $G(\omega_D)$ is elementary abelian of exponent 2 and order 2^l where l is even and that the group $\mathcal{G}/Ker(D)$ is a central extension of $G(\omega_D)$ with kernel $\{\pm 1\}$.

§3. Class two Galois representations in the case of number fields

We recall that the absolute Galois group $\mathcal{G}_k$ of a number field k satisfies the inflation property (1.2). This fact will be used in the following without further mention. The first result in this section is the finiteness result Theorem 1 which was stated in the introduction.

(3.1) **Theorem** *Let* k *be a number field, let* h *be a positive integer and let* S *be a finite set of places containing all places above* h *and infinity. Then there are only finitely many isomorphism classes of class two representations of* $\mathcal{G}_k$ *which are unramified outside* S *and whose characters are rational over* $\mathbb{Q}(W_h)$.

Proof of (3.1): The proof is based on the well known fact that for every positive integer d, for every number field K and every finite set of places S of K which contains all the infinite places of K the degree of the maximal abelian

extension $K^{ab}(S,d)$ of K which is unramified outside S and whose Galois group $G(K^{ab}(S,d)/K)$ has exponent dividing d is bounded from above by a positive integer depending only on K, S and d. The standard proof of this theorem uses basic results of algebraic number theory and is given e.g. in [18], Chapter VIII, Prop. 1.6, p. 194/195. It implies that there are only finitely many symplectic pairings $\omega \in PS(\mathcal{A}_k, \mathbb{C}^*)$ such that the abelian extension K^ω/k is unramified outside S and such that the exponent of the Galois group $G(K^\omega/k)$ divides the number of roots of unity in $\mathbb{Q}(W_h)$. It also shows that for any such ω there are only finitely many central characters χ for ω such that χ is unramified outside the finite set of places of K^ω which extend the places in S and such that all values of χ belong to $\mathbb{Q}(W_h)$. The bijective correspondence between nontrivial central pairs of $\mathcal{G}_k$ and isomorphism classes of class two representations of $\mathcal{G}_k$ which was established in (2.2) implies the assertion.

The following result contains theorem 2 stated in the introduction.

(3.2) **Theorem** *Assume that k is a number field. Then for every nontrivial $\omega \in PS(\mathcal{A}_k, \mathbb{C}^*)$ the genus of class two representations correponding to ω by (2.3) contains a representation D such that its character is rational over $\mathbb{Q}(W_{\overline{b}(\omega)})$. Moreover, if $U(\overline{b}(\omega), S(\overline{b}(\omega))) = (k^*)^{\overline{b}(\omega)}$ then the representation D can be chosen to be unramified outside $S(b(\omega))$.*

Proof: (1.6), (1.7) and (2.4) imply that there is a central character χ for ω of order $\overline{b}(\omega)$, and therefore by (2.2) the character of the representation $D(\omega, \chi)$ is rational over $\mathbb{Q}(W_{\overline{b}(\omega)})$. The last assertion follows from (1.9).

Applying (2.4) to the examples in (1.10) leads to examples of class two representations in the cases $k = \mathbb{Q}$ and $k = \mathbb{Q}(\sqrt[2]{-1})$.

References

[1] E. Artin, J. Tate: Class field theory, Benjamin, New York, 1967

[2] R. Brauer: Über die Konstruktion der Schiefkörper, die von endlichem Rang in bezug auf ein gegebenes Zentrum sind, JRAM, 168, 1932, 44-64

[3] C. Chevalley: Class field theory, Nagoya University, 1954

[4] A.H. Clifford: Representations induced in an invariant subgroup, Annals of Mathematics, 38, 1937, 533-550

[5] M. Deuring: Algebren, Springer Verlag, Berlin, 1935

[6] A. Fröhlich: On fields of class two, Proc. London Math. Soc., 4, 1954, 235-256

[7] K. Hoechsmann: Zum Einbettungsproblem, JRAM, 229, 1967, 81-106

[8] M. Ikeda: Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem, Abh. Math. Seminar der Univ. Hamburg, 24, 1960, 126-131

[9] I.M. Isaacs: Character theory of finite groups, Academic Press, New York, 1976

[10] S. Lang: Elliptic functions, Addison Wesley Publ. Comp., Reading Mass., 1973

[11] J. Neukirch: Über das Einbettungsproblem der algebraischen Zahlentheorie, Inv. Math., 21, 1973, 59-116

[12] H. Opolka: A not on regular crossed products and Galois representations, Comm. in Algebra, 35, 5, 2007, 1469-1478

[13] H. Opolka: Normenreste in relativ abelschen Zahlkörpererweiterungen und symplektische Paarungen, Abh. Math. Sem. Univ. Hamburg, 54, 1984, 1-4

[14] G. Poitou: Cohomologie Galoisienne des modules finis, Dunod, Paris, 1967

[15] M. J. Razar: Central and genus class fields and the Hasse norm theorem, Compositio Math. , 35, 1977, 281-298

[16] J.P. Serre: Modular forms of weight one and Galois representations, in: A. Fröhlich (ed.): Algebraic number fields, Academic Press, New York, 1977, pp. 193-268

[17] S. Shirai: On the decomposition laws of rational primes in certain class 2 extensions, Advanced Studies in Pure Mathematics, 13, 1988, 345-411

[18] J. H. Silverman: The arithmetic of elliptic curves, Springer Verlag, New York, 1986

[19] J.H. Silverman, J. Tate: Rational points on elliptic curves, Springer Verlag, New York, 1992

[20] S.S. Shatz: Profinite groups, arithmetic and geometry, Annals of Mathematics Studies, Princeton University Press, 1972

[21] G. Steinke: Über Auflösungen zahlentheoretischer Knoten, Schriftenreihe des Mathematischen Instituts der Universität Münster, 25, 1982

[22] J. Tate: Duality theorems in Galois cohomology over number fields, Proceedings of the International Congress of Mathematicians, Stockholm, 1962, 288-295

[23] J. Tate: Global class field theory; in: J.W.S. Cassels, A. Fröhlich (eds.): Algebraic number theory, Academic Press, New York, 1967

[24] T. Yamada: The Schur subgroup of the Brauer group, Springer Verlag, LNM 397, Berlin, 1974

[25] K. Yamazaki: On projective representations and ring extensions of finite groups, J. Fac. Sc. Univ. of Tokyo, Sect. 1, 10, 1964, 147-195

Typeset with Scientific Word 3.0 and AMS LaTeX